TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 6, December 2020, pp. 2983~2991
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i6.13746

A new block cipher for image encryption based on multi chaotic systems

Donia Fadhil Chalob, Amal Abdulbaqi Maryoosh, Zainab Mohammed Essa, Elaf Nassir abbud
Department of computer Science, Collage of education, Mustansiyiah University, Iraq

Article Info

Article history:

Received Jul 28, 2019
Revised Mar 5, 2020
Accepted Jun 12, 2020

Keywords:

Arnold cat map
Chaotic
Chen system
Image encryption
Logistic map

ABSTRACT

In this paper, a new algorithm for image encryption is proposed based on three chaotic systems which are Chen system, logistic map and two-dimensional (2D) Arnold cat map. First, a permutation scheme is applied to the image, and then shuffled image is partitioned into blocks of pixels. For each block, Chen system is employed for confusion and then logistic map is employed for generating subsititution-box (S-box) to substitute image blocks. The S-box is dynamic, where it is shuffled for each image block using permutation operation. Then, 2D Arnold cat map is used for providing diffusion, after that XORing the result using Chen system to obtain the encrypted image. The high security of proposed algorithm is experimented using histograms, unified average changing intensity (UACI), number of pixels change rate (NPCR), entropy, correlation and key space analyses.

Corresponding Author:

Amal Abdulbaqi Maryoosh,
Department of computer Science, Collage of education,
Mustansiyiah University,
Baghdad, Iraq.
Email: amalmaryoosh@uomustansiriyah.edu.iq

1. INTRODUCTION

With the fast progress of image transmission through computer networks, particularly the Internet, images security has turned into a main issue. Image encryption, specifically, is critically required yet it is a challenging task—it is totally not the same as text encryption due to some the inherent features of an image, for example, tremendous data bulk and highly redundant, they are for the most part difficult to deal with by utilizing traditional algorithms [1]. To achieve a secure encryption method, two basic characteristics must be followed. The first is the confusion feature which necessitates that, encrypted text should has arbitrary appearance, which means that the pixel values uniformly distributed. The second is the diffusion feature that should create totally unlike encrypted text by similar keys for the equivalent original text. The secure transmission of color images through public channel, chaotic systems that fulfill the main prerequisites of confusion and diffusion are distinguished based on their reactive to control parameters and initial conditions, pseudorandomness and ergodicity. Exploiting these favorable features, chaos-based algorithms have revealed superior characteristics in complexity and security [2, 3].

Several studies are related to this work, Z. l. Zhu *et al.* [4] suggested an image encryption algotithm utilizing logistic map for diffusion and Arnold cat map for bit- level permutation. M. J. Rostami *et al.* [5] employed logistic map for the encryption of gray-scale image, divides the image into blocks and encrypts them with XOR operation and chaotic windows. W. Zhang *et al.* [6] a three-dimensional bit matrix permutation is proposed, via gathering features of Chen system with a three-dimensional cat map in permutation operation, a double random place bit-level permutation in three-dimensional (3D) matrix is developed. Liu and Miao [7]

proposed a new image encryption algorithm based on parameter-varied logistic chaotic map to shuffle the plain image and dynamical algorithm to encrypt the image. L. Xu *et al.* [8] presents a new bit-level algorithm of image encryption that depends on piecewise linear chaotic maps (PWLCM), diffuse the image sequences via a new diffusion strategy.

Then, the control of a chaotic map is utilized for swapped the binary elements in the sequences, which permute bits in particular bitplane into another bitplane. X. Wang *et al.* [9] suggests a method for block image encryption depended on hybrid chaotic maps and dynamic random growth technique. In diffusion operation, an intermediary parameter is determined by the image block. The intermediary parameter is utilized as the initial parameter of chaotic cat map in order to generate a random key stream. Suryadi M. T. *et al.* [10] built a chaotic encryption scheme for digital image by utilizing logistic map for key stream as a random number generator. Xiuli Chai *et al.* [11] introduced a scheme for image encryption depended on the memristive chaotic system, compressive sensing and elementary cellular automata. Wavelet coefficients of an original image are permuted using the zigzag path and elementary cellular automata. After that, the compressive sensing is utilized to compress and encrypt the permuted image. Hash value of SHA 512 of plain image is used to gain some parameters utilized in encryption operation. Hongyao Deng *et al.* [12] proposed a chaos-based image encryption algorithm, by shuffle to mask original organization of the pixels in images using cat map and diffusion to mask their values using logistic map. Salah T. Allawi [13] presented a new method to encrypt RGB image by dividing the image into two equal parts, encrypting each part using a secret key generated by one-dimensional (1D) logistic mapping and permutation the pixels position using random numbers generated by using linear-feedback shift registers (LFSRs). Pan *et al.* [14] studied the digital image encryption technology with the dual logistic chaotic map as a tool. Ye, G., & Huang [15] presented a chaotic image encryption algorithm by using SHA-3 hash function, cat map, logistic map and auto-updating system. At the same time, for various rounds of iteration and various images, the algorithm demonstrates like one-time pad. Ye, G. *et al.* [16] presented method includes permutation, modulation and diffusion processes. This technique overcomes the drawback in traditional methods of strictly permuting the places of pixels before diffusion. Information entropy is utilized to effect the keystream generation. Zhang Y. [17] suggested a plaintext-related image encryption algorithm depended on hyper chaotic Lorenz system, six pseudorandom matrices are generated using the hyper chaotic Lorenz system, such that, two of the matrices utilize add-modulus operations to diffuse the plaintext unrelated image, other four matrices confuse the plaintext related image. N. Oussama *et al.* [18] designed a novel symmetric image encryption method based on polar decomposition of matrices and 1D logistic map.

In this paper, a new block algorithm for color image encryption is suggested based on three chaotic systems to overcome the problem of high computation, pattern appearance issue and so slow when using traditional algorithms image encryption. High confusion is provided by chaotic system and dynamic S-box and high diffusion is provided by permutation methods to increase the security and efficiency of image encryption. This paper results are experimented by information entropy, correlation, histogram, NPCR, UACI and key space. The experimental results show that the proposed scheme efficient and more secure for image encryption. The rest of this paper is organized as follows. In section 2, the methods that used in the proposed algorithm are introduced. The suggested scheme in details is presented in section 3. Then, security experiments with comparison are achieved in section 4 to show the effectiveness of our scheme. Finally, some conclusions that extracted from this work are in section 5.

2. CHAOTIC SYSTEMS

The proposed algorithm employs three chaotic maps in this paper, namely Chen system [19], one-dimensional (1D) logistic map [20] and two-dimensional (2D) Arnold cat map [21].

2.1. Chen system

Chen chaotic system [19] is expressed by in (1):

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \quad (1)$$

where a = 35, b = 3 and c = 28 are parameters, x, y, z are state variables. The attractor and phase diagram of Chen system are illustrated in Figures 1 (a) and (b), respectively.

2.2. Logistic map

In 1845, Pierre Verhulst suggested logistic map, that's a simple and popular chaotic map. When used in 1979 via the biologist Robert M. May, logistic map became very common. Where the equation of one dimensional logistic map is shown in (2):

$$x_{n+1} = \mu \times x_n \times (1 - x_n) \quad (2)$$

In which $x_n \in [0,1]$, x_0 denotes the initial condition and μ is a constant parameter between 0 and 4. For $(3.5699 < \mu \leq 4)$, in (2) shows a chaotic behavior [20]. By reason of its simplicity and high efficiency, this paper employed the chaotic systems times in its algorithm.

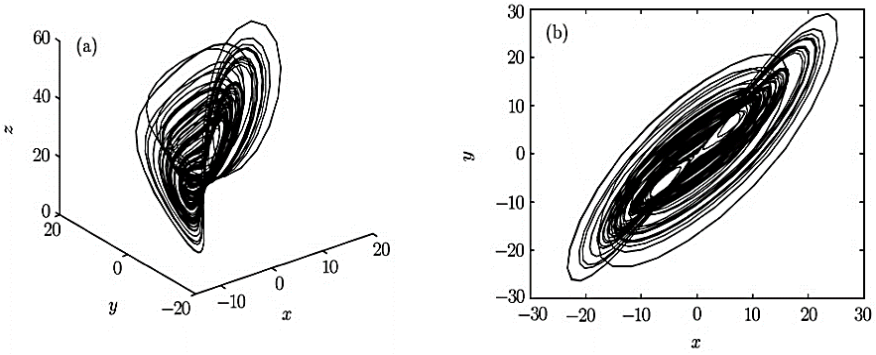


Figure 1. Chaotic attractor; (a) Chen attractor 3-D, (b) phase diagram (x-y)

2.3. Arnold cat map

The classic Arnold cat map is an invertible chaotic map of two dimensions [21] described via in (3):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \quad (3)$$

where x_n, y_n are the position in the matrix of samples (N×N), n=1,2,3,…, N-1 and x_{n+1}, y_{n+1} are the position transformed after cat map. The map is recognized to become chaotic, by explanation of geometry displayed in Figure 2, where one can notice that a square unit is at the beginning stretched by means of linear transformation and then folded through mod, modulo operation.

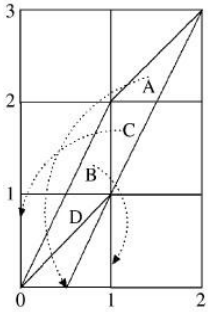


Figure 2. Geometric explanation of 2D cat map

3. PROPOSED ALGORITHM

The encryption algorithm contains three main operations, which are: permutation, substitution and add chaotic keys. At first, the plain image will be input to permutation step and then the permuted image will be divided into 4x4 blocks to be entered to n iterations of add Chen key, then substitution which is done by generating dynamic S-box using logistic map. After the end of iterations the resulting image will be permuted using Arnold cat map to increase the diffusion. Finally, XORed the resulted image with Chen key which provide extra confusion process. The general structure diagram of suggested algorithm shown in Figure 3.

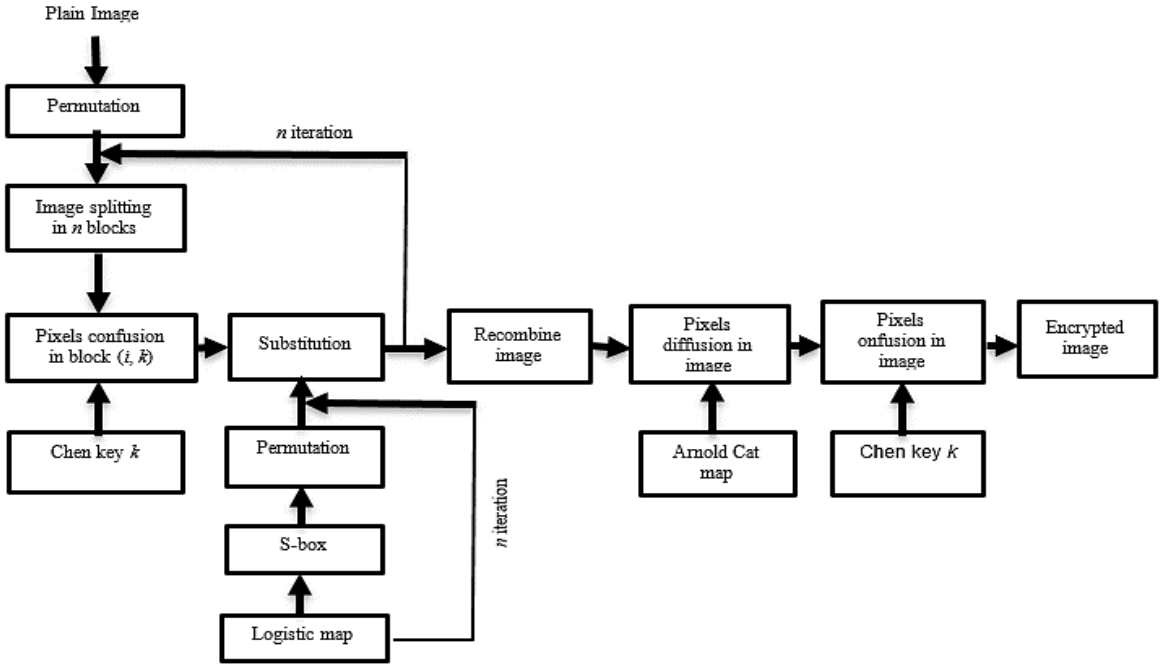


Figure 3. General structure of proposed algorithm

3.1. Permutation method

In order to achieve the permutation technique of cryptosystems, scrambleness behavior is required. In this algorithm, two permutation methods are used for providing a high level of diffusion. In this method we relied on scrambling rows and columns based on sum invariance of row and column through circular shift process. In the beginning we shifts each row in image by the total sum of the row and column's pixel values and save the result image in a variable, and then transpose the resulting image and implement the same method in each column on the transposed image. Table 1 shown the random swap of 10x10 ladybug sub image pixels. Figure 4 shown the plain ladybug image and the resulting image after permutation.

Table 1. Original pixel location on left and their new position on right

The random swap of 10x10 ladybug sub image pixels	
86 85 80 81 73 76 77 121 126 33	97 45 254 125 187 121 89 121 98 222
99 98 98 97 93 89 125 164 151 103	99 75 77 191 175 200 231 124 255 197
120 124 113 118 99 125 175 204 192 177	245 123 162 151 241 103 164 80 73 172
126 117 123 108 132 179 215 212 200 184	162 118 126 206 192 120 203 249 179 104
121 117 123 121 181 222 231 222 203 168	225 132 217 86 33 85 177 245 240 117
112 122 91 167 223 245 240 225 180 172	251 255 12 97 99 213 126 125 212 113
104 75 94 202 252 255 240 193 165 208	208 169 27 94 179 202 98 240 165 81
102 27 165 239 252 254 214 162 197 239	102 193 91 121 165 252 247 204 168 93
45 97 213 249 254 240 162 191 251 217	122 243 108 223 167 76 239 180 112 222
12 179 247 255 245 187 169 241 243 206	123 239 181 240 252 215 254 184 117 214

(a) (b)

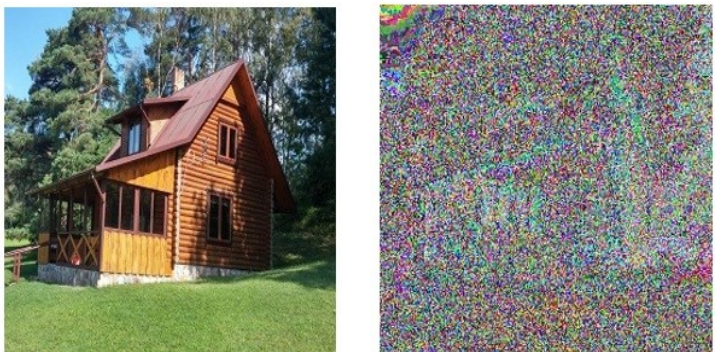
Figure 4. (a) Plain ladybug image, (b) permuted ladybug image

3.1.1. Permutation algorithm

Input: plain image (m)
Output: permuted image (p1)
Step1: read plain image(m)
Step2: for col1 ←1: size (m)
I1← circular_shift (sum (m (column)))
end
Step3: for row1←1: size (m)
I2← circular_shift (sum (m (row)))
end
Step4: transpose(I2)
Step5: for col2 ←1: size (m)
I3← circular_shift (sum (m (column)))
end
Step6: for row2←1: size (m)
I4← circular_shift (sum (m (row)))
end
Step7: p1← I4

3.2. Substitution

In this process, this paper generates a dynamic S-box using logistic map and improve the key sensitivity by implementing the proposed permutation method on the S-box in each round, where each block will be substituted with a new S-box, this operation will provide one time pad property. Figure 5 demonstrates the result of encryption house image by using dynamic S-box only.



(a) (b)

Figure 5. (a) Plain house image, (b) image after substitution process

3.3. Encryption algorithm

Input: permuted image (p1), Chen_key, Logistic parameters(x,n,r0) block size(z)
Output: encrypted image (c)
Step1: read permuted image (p1)
Step2: k1 ← XOR(p1, Chen_key)
Step3: Sbox ←Logistic_map(x,n,r0)
for j ← 1:z
sub_byte← permutation (Sbox)
s← sub_byte (p)
end
Step4: p2 ← Aronld cat_map(s)
Step5: k2 ← xor (Chen_key, p2)
Step6: c ← k2

3.4. Decryption algorithm

Input: encrypted image (c), Chen_key, Inv_Logistic parameters(x1,n1,r0) block size(z)
Output: plain image (m)

```
Step1: read encrypted image (c)
Step2: k2 ← xor (Chen_key, c)
Step3: p2 ← Aronld cat_map(k2)
Step4: Inv_ Sbox ← Inv_Logistic_map(x1,n1,r0)
       for j ← 1:z
            Inv_ sub_byte← Inv_ permutation (Inv_Sbox)
             s← Inv_sub_byte (p2)
         end
Step5: k1 ← XOR(s, Chen_key)
Step6: m ← k1
```

4. SECURITY ANALYSIS

The results of series of tests are reviewed in this section to illustrate the effectiveness of the suggested algorithm. The valuation is made up of various practical experiments. At the end of this section, a comparison is made between the proposed algorithm and in [17]. The experiments are performed via Matlab R2013a on a computer with Intel Core i3 CPU 2.10 GHz, 3 GB of RAM.

4.1. Histogram analysis

Histogram analysis is used to explain the confusion and diffusion characteristic of the encryption algorithm. Figure 6 shown the difference in image distribution among plain flower image, its permutation and encryption.

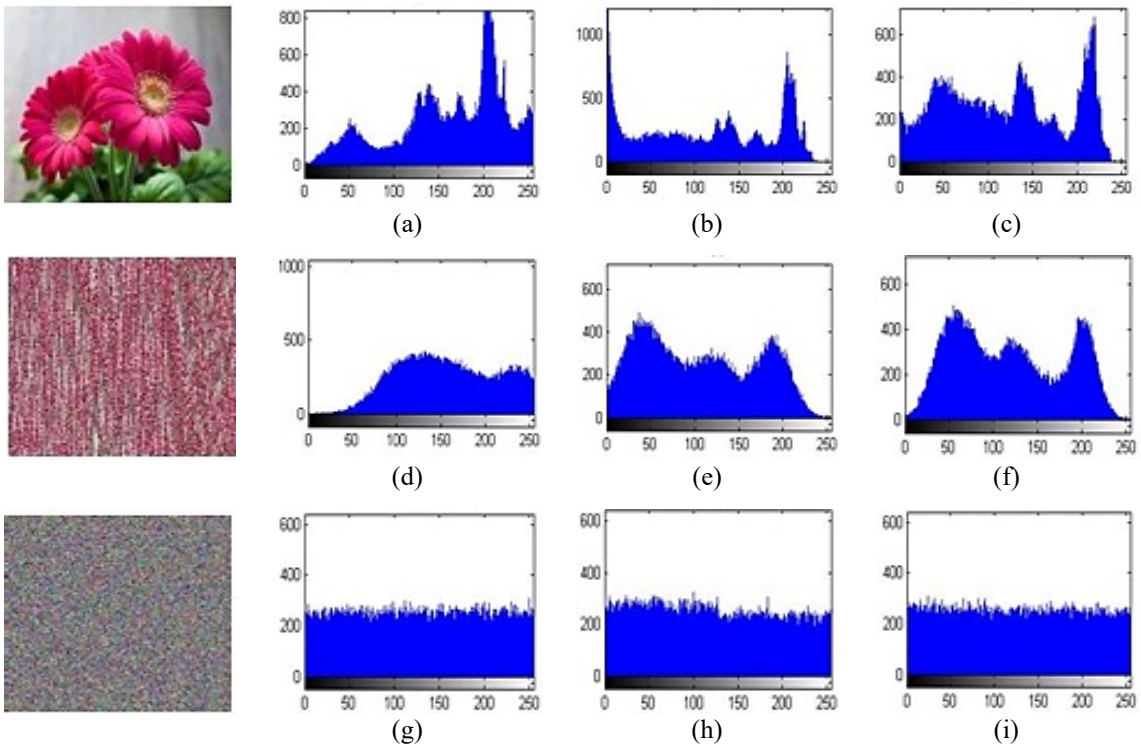


Figure 6. Histogram analysis; (a), (b) and (c) histogram plain flower image of RGB, (e) and (f) are histogram permuted image of RGB, (g), (h) and (i) are histogram encrypted image of RGB

4.2. Correlation coefficients analysis

Every pixel is extremely associated with its neighboring pixels in the image data [22]. A typical encryption algorithm should output cipher image in the neighboring pixels without such a correlation. In horizontal, diagonal and vertical orientations, the correlation between two neighboring pixels is studied by following equations:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (4)$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N} x_j)^2, \quad (5)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N} x_j)\,(y_j - \frac{1}{N}\sum_{j=1}^{N} y_j). \quad (6)$$

x and y are two adjacent pixel intensity values in an image, N is the number of neighboring pixels chosen from the image to determine the correlation. The results of correlation of various encrypted images are displayed in Table 2.

Table 2. Correlation coefficients of two neighboring pixels in encrypted images of proposed algorithm

Images	Correlation of Proposed Algorithm		
	Vertical	Horizontal	Diagonal
House	-0.0089	-0.0049	-0.0125
Flower	-0.0041	-0.0038	0.0034
Pepper	0.0020	-0.0035	0.0016
Lion	-0.0018	-0.0025	0.0026
Bird	-0.0027	0.0028	0.0030
Garden	-0.0020	0.0039	0.0033
Horse	0.0060	-0.0036	-3.1399e-04
Sky	-0.0030	-0.0024	0.0021
Ladybug	-0.0037	0.0074	-0.0021
Splash	-0.0062	0.0020	-0.0036

4.3. Information entropy analysis

Information entropy evaluates uncertainty of a random variable as following [23]:

$$E = \sum_{i=1}^{256} P(i) \log\left(\frac{1}{P(i)}\right), \quad (7)$$

where P(i) is the eventuality presence of pixel i. A larger entropy value denotes a bigger security level that used to assess the images encryption. Commonly, an entropy value so close to the typical value of 8 is regarded secure from a brute force attack. The values of information entropy that obtained from proposed algorithm are closer to 8, this shows that the proposed method has good random. Table 3 shows the values of information entropy for the various plain images and encrypted images.

Table 3. Information entropy of plain and encrypted image of proposed algorithm

Images	Entropy of plain images	Entropy of proposed system
House	7.7871	7.9990
Flower	7.7666	7.9991
Pepper	7.7124	7.9989
Lion	7.8794	7.9989
Bird	7.6741	7.9977
Garden	7.7955	7.9990
Horse	7.6143	7.9988
Sky	7.9339	7.9990
Ladybug	7.5706	7.9990
Splash	7.3795	7.9990

4.4. Analysis of resisting differential attacks

Differential attack studies how a minor changing in an original image is able to influence corresponding encrypted image. A typical encryption algorithm have to be able to withstand differential attack, which means, any tiny change (even if changed a bit) in an original image will lead in a totally different encrypted image. Number of pixels change rate (NPCR) and unified average changing intensity (UACI), described by in (8) and (9), are two of the most common indicators to determine the competence of differential attacks resisting in encrypted image [24]:

$$NPCR = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} d_{ij} \times 100\%, \quad (8)$$

$$UACI = \frac{1}{255 \times W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left| C_{ij}^{1} C_{ij}^{2} \right| \times 100\%, \quad (9)$$

where H and W refer to the height and width of the encrypted images, C^1 and C^2 are two cipher images and d_{ij} is defined by in (10):

$$d_{ij} = \begin{cases} 0, & C_{ij}^{1} = C_{ij}^{2}, \\ 1, & C_{ij}^{1} \neq C_{ij}^{2}. \end{cases} \quad (10)$$

The typical value of NPCR and UACI are 99.61 and 33.46 [7]. This paper implemented NPCR and UACI measures on ten color images and the two indicator results are close to the optimal value. Table 4 shown the results of NPCR and UACI in proposed scheme.

Table 4. UACI and NPCR indicator of encrypted image of proposed algorithm

Images	Proposed Algorithm	
	UACI	NPCR
House	32.09	99.58
Flower	33.74	99.64
Pepper	33.86	99.61
Lion	33.57	99.61
Bird	33.92	99.61
Garden	33.41	99.61
Horse	33.41	99.61
Sky	33.80	99.60
Ladybug	34.07	99.61
Splash	33.58	99.62

4.5. Key space analysis

The encryption algorithm contains the keys: 1) initial values of x, y, z and x0 ; 2) control parameter of a, b, c and μ. In general, the valid precision of the initial conditions could be set to 10^{-14} for continuous chaotic system exhibited as nonlinear differential equation. Thus, the size of key space could reach $2^{112} > 2^{100}$ [25]. Thus, it is noticed that the value of the chaos system key space is much larger and the proposed algorithm can highly resist against brute-force attacks. Table 5 demonstrates the results of Pepper image encrypted using proposed algorithm and in [17].

Table 5. Comparison results of proposed algorithm with [17]

Test	Proposed Algorithm	[17]
Correlation Coefficients	V 0.0020	V 0.013633
	H -0.0035	H -0.003522
	D 0.0016	D 0.007701
Entropy	7.9989	7.9992
NPCR	99.61	99.60
UACI	33.86	33.48

5. CONCLUSION

In this paper, a new block image encryption algorithm has been introduced to provide high level of security for color image encryption on the basis of the combination of permutation method, chaotic systems and dynamic S-box. Whereas the random permutation and Arnold cat map scrambling provide high level of diffusion, the substitution process provide high confusion using Chen system and improve the key sensitivity by generating a one-time S-box using logistic map. Also, the use of chaotic system offer high randomness, large key space, key sensitivity and confusion. The effectiveness of this algorithm has been confirmed through above experiment results. According to these results, the proposed algorithm offers high resistance against statistical and differential attacks.

ACKNOWLEDGEMENTS

We would like to thank Mustansiriyah university (www.uomustansiriyah.edu.iq), Baghdad, Iraq for its support in the present work.

REFERENCES

[1] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514-522, 2011.

[2] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion–substitution based gray image encryption scheme," *Digital Signal Processing*, vol. 23, no. 3, pp. 894-901, 2013.

[3] I. Hussain, T. Shah, and M. A. Gondal, "Application of S -box and chaotic map for image encryption," *Mathematical and Computer Modelling*, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[4] Z. Zhu, W. Zhang, K. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171-1186, 2011.

[5] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-pour, "A novel parallel image encryption with chaotic windows based on Logistic map," *Computers and Electrical Engineering*, vol. 62, pp.3 84-400, 2017.

[6] W. Zhang, H. Yu, Y. Zhao, Z. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36-50, 2016.

[7] L. Liu, and S. Miao, "A new image encryption algorithm based on Logistic chaotic map with varying parameter," *SpringerPlus*, vol. 5, no. 1, 2016.

[8] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps", *Optics and Lasers in Engineering*, vol. 78, pp. 17-25, 2016.

[9] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10-18, 2015.

[10] Suryadi M. T., E. Nurpeti, and D. Widya, "Performance of Chaos-Based Encryption Algorithm for Digital Image," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 12, no. 3, pp. 675-682, 2014.

[11] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124-144, 2018.

[12] Hongyao Deng, Qingxin Zhu, Xiuli Song and Jingsong Tao, "Chaos-Based Image Encryption Algorithm Using Decomposition," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 12, no. 1, pp. 575-583, 2014.

[13] Salah T. Allawi, "Image Encryption Based on Chaotic Mapping and Random Numbers," *Journal of Engineering and Applied Sciences*, vol. 14, no. 19, pp. 6954-6958, 2019.

[14] H. Pan, Y. Lei, and C. Jian, "Research on digital image encryption algorithm based on double Logistic chaotic map," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 142, 2018.

[15] G. Ye, and X. Huang, "A secure image encryption algorithm based on chaotic maps and SHA-3," *Security and Communication Networks*, vol. 9, no. 13, pp. 2015-2023, 2016.

[16] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A Chaotic Image Encryption Algorithm Based on Information Entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 1, pp. 1-11, 2018.

[17] Y. Zhang, "A Chaotic System Based Image Encryption Algorithm using Plaintext-related Confusion," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 12, no. 11, pp. 7952-7962, 2014.

[18] N. Oussama, B. Assia, and N. Lemnouar, "Secure image encryption scheme based on polar decomposition and chaotic map," *International Journal of Information and Communication Technology*, vol. 10, no. 4, pp. 437-453, 2017.

[19] H. Dai, L. X. Jia, M. Hui, and G.-Q. Si, "A new three-dimensional chaotic system and its modifed generalized projective synchronization," *Chin. Phys. B*, vol. 20, no. 4, pp. 1-10, 2011.

[20] J. A. P. Artiles, D. P. B. Chaves and C. Pimentel, "Image encryption using block cipher and chaotic sequences," *Signal Processing: Image Communication*, vol. 79, pp. 24-31, 2019.

[21] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[22] R. Sridevi, P. Philominathan, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Logistic and Standard Coupled Mapping on Pre and Post Shuffled Images: A Method of Image Encryption," *Asian J. Sci. Res,* vol. 10, no. 1, pp. 10-23, 2017.

[23] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map," *Entropy*, vol. 21, no. 7, pp. 1-17, 2019.

[24] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes," *Entropy*, vol. 21, no. 3, pp. 1-21, 2019.

[25] H. Liu, A. Kadir, and P. Gong, "A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise," *Optics Communications*, vol. 338, pp. 340-347, 2015.